

On the Construction of Nonbinary Quantum BCH Codes

Giuliano G. La Guardia

Abstract—Four quantum code constructions generating several new families of good nonbinary quantum nonprimitive non-narrow-sense Bose-Chaudhuri-Hocquenghem (BCH) codes are presented in this paper. The first two ones are based on Calderbank-Shor-Steane (CSS) construction derived from two nonprimitive BCH codes, not necessarily self-orthogonal. The third one is based on nonbinary Steane's enlargement of CSS codes applied to suitable sub-families of nonprimitive non-narrow-sense BCH codes. The fourth construction is derived from suitable sub-families of Hermitian self-orthogonal nonprimitive non-narrow-sense BCH codes. These constructions generate new families of quantum BCH codes whose parameters are better than the ones available in the literature.

I. INTRODUCTION

Constructions of quantum codes with good parameters are much investigated in the literature [1, 3, 6–11, 13–17, 20, 21]. The CSS construction, the Hermitian as well as the symplectic construction are the most utilized construction methods in order to generate good quantum codes.

In [1], the authors constructed families of good nonbinary quantum (narrow-sense) BCH codes by showing useful properties of cyclotomic cosets. More specifically, they computed the exact dimension of classical narrow-sense BCH codes of length n with minimum distance of order $O(n^{1/2})$ as well as they have established useful conditions to provide dual containing (Euclidean as well as Hermitian) BCH codes. Following this approach, the authors of [17] also have constructed quantum BCH codes by using self-orthogonal codes. In [14, 15], new families of nonbinary quantum BCH codes were constructed by means of the CSS, Hermitian and also by using the Steane's construction applied to suitable sub-families of BCH codes. Finally, new quantum MDS codes of non Reed-Solomon type are constructed in [16].

Motivated by the construction of new nonbinary quantum BCH codes with good parameters, we propose four quantum code constructions generating new families of good codes. These new families consist of quantum BCH codes whose parameters are better than the ones available in the literature. In other words, fixing n and d , the new quantum BCH codes achieve greater values of the number of qudits than the codes available in the literature (see Tables I–VI in pages 8–9).

In order to construct these new families it is necessary to know the exactly dimension of the classical BCH codes used for this purpose. This is a difficult task since the dimension of BCH codes is not known. To solve this problem, we show suitable properties of cyclotomic cosets providing the exact

dimension and great minimum distance for the corresponding quantum codes as in the Euclidean as well as in the Hermitian case. Additionally, by applying the concept of linear congruence, we prove (for codes of prime length) the existence of, at least, one q -ary coset containing two consecutive integers. By means of this result we also construct new families of good nonbinary quantum BCH codes, since this technique allows the construction of quantum codes with great dimension and great minimum distance.

The proposed families have parameters

- $[[n, n - 4(c - 2) - 2, d \geq c]]_q$,

where $q \geq 4$ is a prime power, n is an integer such that $\gcd(q, n) = 1$, $(q - 1) \mid n$, $m = \text{ord}_n(q) = 2$ and $2 \leq c \leq r$, where r is such that $n = r(q - 1)$;

- $[[n, n - 2mr, d \geq r + 2]]_q$,

where $m = \text{ord}_n(q) \geq 2$, n is a prime number and r is the number of cosets satisfying suitable conditions (see Theorem 3.4);

- $[[n, n - m(2r - 1), d \geq r + 2]]_q$,

where $m = \text{ord}_n(q) \geq 2$, n is a prime number and $q \geq 3$;

- $[[n, n - 4c, d \geq c + 2]]_q$,

where $n > q$ is an integer with $\gcd(q, n) = 1$, $(q - 1) \mid n$, $m = \text{ord}_n(q) = 2$, $1 \leq c \leq r - 3$ and $r > 3$ is such that $n = r(q - 1)$;

- $[[n, n - 4c - 2, d \geq c + 2]]_q$,

where $2 \leq c \leq r - 2$, $q > 3$, $n = r(q^2 - 1)$, $r > 1$ and $m = \text{ord}_n(q^2) = 2$;

- $[[n, n - 2mr, d \geq r + 2]]_q$,

where $q \geq 3$ is a prime power, $n > q^2$ is a prime number such that $\gcd(q, n) = 1$, $m = \text{ord}_n(q^2) \geq 2$ and r is the number of cosets satisfying suitable conditions (see Theorem 3.9).

This paper is structured as follows. In Section II we recall basic concepts on cyclic codes. In Section III, the four new quantum code constructions are presented. More precisely: in Subsection III-A, new families of nonprimitive quantum codes of length n , where $m = \text{ord}_n(q) = 2$, are generated; in Subsection III-B, new families of q -ary quantum nonprimitive non-narrow-sense BCH codes of prime length, where $m = \text{ord}_n(q) \geq 2$, are constructed; in Subsection III-C, new families of quantum codes derived from nonbinary Steane's construction applied to nonprimitive non-narrow-sense Euclidean self-orthogonal BCH codes are shown; in Subsection III-D, the construction of new families of quantum codes derived from nonprimitive non-narrow-sense Hermitian self-orthogonal BCH codes are proposed. In Section IV, the parameters of the new quantum BCH codes are compared with the ones available in the literature. Finally, in Section V, a summary of this paper is given.

II. REVIEW OF CYCLIC CODES

This section presents some basic concepts on cyclic codes, necessary for the development of this paper. For more details, we refer the reader to [18].

Throughout this paper, $p \neq 2$ denotes a prime number, $q \neq 2$ is a prime power, F_q is the finite field with q elements, n is the code length (we always consider that $\gcd(n, q) = 1$). If C is an $[n, k, d]_q$ code then C^\perp denotes its Euclidean dual and C^{\perp_H} denotes its Hermitian dual. As usual, $m = \text{ord}_n(q)$ denotes the multiplicative order of q modulo n and $\mathbb{C}_{[s]}$ denotes the q -ary cyclotomic coset modulo n containing s , defined by $\mathbb{C}_s = \{s, sq, sq^2, sq^3, \dots, sq^{m_s-1}\}$ (m_s is the smallest positive integer such that $sq^{m_s} \equiv s \pmod{n}$), where s is not necessarily the smallest number in the coset $\mathbb{C}_{[s]}$. The minimal polynomial over F_q of $\beta \in F_{q^m}$ is the monic polynomial of smallest degree, $M(x)$, with coefficients in F_q such that $M(\beta) = 0$. If $\beta = \alpha^i$ for some primitive n th root of unity $\alpha \in F_{q^m}$ then the minimal polynomial of $\beta = \alpha^i$ is denoted by $M^{(i)}(x)$. It is well known that $x^n - 1 = \prod_s M^{(s)}(x)$, where

$M^{(s)}(x)$ denotes the s -th minimal polynomial of $\alpha^s \in F_{q^m}$ over F_q , and s runs through the coset representatives mod n . Let C be a cyclic code of length n . Then there is only one monic polynomial $g(x)$ with minimal degree in C such that $g(x)$ is the generator polynomial of C , where $g(x)$ is a factor of $x^n - 1$. The dimension of C equals $n - \deg g(x)$. The (Euclidean) dual code C^\perp of a cyclic code is cyclic and has generator polynomial $g(x)^\perp = x^{\deg h(x)} h(x^{-1})$, where $h(x) = (x^n - 1)/g(x)$. Thus, the code having generator polynomial $h(x)$ is equivalent to the dual code C^\perp .

Theorem 2.1: [18, pg. 201] (The BCH bound) Let C be a cyclic code with generator polynomial $g(x)$ such that, for some integers $b \geq 0$, $\delta \geq 1$, and $\alpha \in F_{q^m}$ (α is a primitive element of F_{q^m}), we have $g(\alpha^b) = g(\alpha^{b+1}) = \dots = g(\alpha^{b+\delta-2}) = 0$, that is, the code has a sequence of $\delta - 1$ consecutive powers of α as zeros. Then the minimum distance of C is, at least, δ .

Definition 2.1: [18, pg. 202] A cyclic code of length n over F_q is a BCH code of designed distance δ if, for some integer $b \geq 0$ we have

$$g(x) = \text{l.c.m.}\{M^{(b)}(x), M^{(b+1)}(x), \dots, M^{(b+\delta-2)}(x)\},$$

that is, $g(x)$ is the monic polynomial of smallest degree over F_q having $\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+\delta-2}$ as zeros.

If $n = q^m - 1$ then the BCH code is called primitive and if $b = 1$ it is called narrow-sense. From the BCH bound, the minimum distance of a BCH code is greater than or equal to its designed distance δ . In this paper we only consider nonprimitive BCH codes.

Bose-Chaudhuri-Hocquenghem (BCH) codes [4, 5, 12] are a well-known class of classical codes. Interesting works concerning the dimension of BCH codes of length n with minimum distance $d = \mathcal{O}(n^{1/2})$ as well as sufficient condition (in some cases, necessary and sufficient condition) for dual (Euclidean and Hermitian) containing BCH codes are presented [1, 17, 22].

III. CODE CONSTRUCTIONS

In this section we present our contributions, that is, the four quantum code constructions previously mentioned. The new families of BCH-CSS codes have parameters better than the ones available in the literature; the new families of BCH-Hermitian codes have parameters better than ones shown in the literature, and the new families of quantum BCH codes derived from q -ary Steane's construction have parameters better than the parameters of the quantum BCH codes generated by applying the q -ary Steane's construction to (classical) BCH codes available in the literature. We recall that in this paper we only consider nonprimitive BCH codes.

A. Construction I - Nonprimitive Codes

In this subsection we construct new families of nonbinary CSS codes derived from two distinct classical BCH codes, not necessarily self-orthogonal. The main result is Theorem 3.1. To proceed further, let us recall the so-called CSS construction:

Definition 3.1: [6, 13, 19, 20] Let C_1 and C_2 denote two classical linear codes with parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$, respectively, such that $C_2 \subset C_1$. Then there exists an $[[n, K = k_1 - k_2, d]]_q$ quantum code, where $d = \min\{wt(c) \mid c \in (C_1 \setminus C_2) \cup (C_2^\perp \setminus C_1^\perp)\}$.

We start by showing Lemma 3.1:

Lemma 3.1: Let $q \geq 3$ be a prime power and $n > q$ be an integer such that $\gcd(q, n) = 1$. Assume also that $(q - 1) \mid n$ and $m = \text{ord}_n(q) \geq 2$ hold. Then each one of the q -ary cyclotomic cosets $\mathbb{C}_{[lr]}$, where r is such that $n = r(q - 1)$ and $1 \leq l \leq q - 2$ is an integer, has only one element.

Proof: Since $rq = n + r$ holds, one has $(lr)q = l(n + r) \equiv lr \pmod{n}$, and therefore $(lr)q^t \equiv lr \pmod{n}$, for each $1 \leq t \leq m - 1$, proving the lemma. ■

To show how Lemma 3.1 works for constructing quantum codes we present an illustrative example:

Example 3.1: Let $q = 7$ and $n = 18$; so one has $m = 3$. Listing the cyclotomic cosets necessary for this construction: $\mathbb{C}_0 = \{0\}$, $\mathbb{C}_1 = \{1, 7, 13\}$, $\mathbb{C}_2 = \{2, 14, 8\}$, $\mathbb{C}_3 = \{3\}$, $\mathbb{C}_4 = \{4, 10, 16\}$, $\mathbb{C}_5 = \{5, 17, 11\}$, $\mathbb{C}_6 = \{6\}$, $\mathbb{C}_9 = \{9\}$, $\mathbb{C}_{12} = \{12\}$ and $\mathbb{C}_{15} = \{15\}$. In this case one has $q - 1 = 6$, $n = 18$ and $r = 3$. If we choose C_1 be the cyclic code generated by the product of the minimal polynomials $M^{(0)}(x)M^{(1)}(x)$ and C_2 as the code generated by the product of the minimal polynomials $\prod_i M^{(i)}(x)$, where $i \notin \{3, 4\}$ and i runs through

the coset representatives mod 18 one has an CSS code with parameters $[[18, 10, d \geq 3]]_7$. Similarly one can get quantum codes with parameters $[[18, 4, d \geq 4]]_7$ $[[18, 2, d \geq 5]]_7$.

Lemma 3.1 can be applied in order to show Theorem 3.1, one of the main results of this subsection:

Theorem 3.1: Suppose that $q > 3$ is a prime power and $n > q$ is an integer such that $\gcd(q, n) = 1$. Assume also that $(q - 1) \mid n$ and $m = \text{ord}_n(q) = 2$ hold. Then there exist quantum codes with parameters $[[n, n - 4(r - 2) - 2, d \geq r]]_q$, where r is such that $n = r(q - 1)$.

Proof: Let C_1 be the cyclic code generated by the product of the minimal polynomials

$$M^{(0)}(x)M^{(1)}(x) \dots M^{(r-2)}(x)$$

and C_2 be the cyclic code generated by $g_2(x)$, that is the product of the minimal polynomials

$$g_2(x) = \prod_i M^{(i)}(x),$$

where $i \notin \{r, r+1, \dots, 2r-2\}$ and i runs through the coset representatives mod n .

Since it is true that $n \mid (q^2 - 1)$ and because we consider only nonprimitive BCH codes then it follows that $r \leq q$. Since $\gcd(q, n) = 1$ one has $r < q$, so the inequalities $(r-2)q < n$ and $r + (r-2)q < n$ hold. We next show that all the q -ary cosets (modulo n) given by $\mathbb{C}_{[0]} = \{0\}$, $\mathbb{C}_{[1]} = \{1, q\}$, $\mathbb{C}_{[2]} = \{2, 2q\}$, $\mathbb{C}_{[3]} = \{3, 3q\}$, \dots , $\mathbb{C}_{[r-2]} = \{r-2, (r-2)q\}$, $\mathbb{C}_{[r]} = \{r\}$, $\mathbb{C}_{[r+1]} = \{r+1, r+q\}$, $\mathbb{C}_{[r+2]} = \{r+2, r+2q\}$, \dots , $\mathbb{C}_{[2r-2]} = \{2r-2, r+(r-2)q\}$, are mutually disjoint and, with exception of the cosets $\mathbb{C}_{[0]} = \{0\}$ and $\mathbb{C}_{[r]} = \{r\}$, each of them has exactly two elements.

The cosets $\mathbb{C}_{[0]}$ and $\mathbb{C}_{[r]}$ have only one element. Let us show that each one of the other cosets has exactly two elements. Since $(r-2)q < n$, then the congruence $l \equiv lq \pmod n$ implies that $l = lq$, where $1 \leq l \leq r-2$, which is a contradiction. If $r+s \equiv (r+s)q \pmod n$, where $1 \leq s \leq r-2$, then $r+s = r+sq$, which is a contradiction.

From now on, we show that all these cosets given above and $\mathbb{C}_{[0]}$ and $\mathbb{C}_{[r]}$ are mutually disjoint. We only consider the case $\mathbb{C}_{[r+l]} = \mathbb{C}_{[r-s]}$, where $1 \leq l, s \leq r-2$, since the other cases are similar to this one. Seeking a contradiction, we assume that $\mathbb{C}_{[r+l]} = \mathbb{C}_{[r-s]}$, where $1 \leq l, s \leq r-2$. If the congruence $(r+l) \equiv (r-s) \pmod n$ holds, one obtains

$$(r+l) \equiv (r-s) \pmod n \implies n \mid (l+s).$$

If $l+s \neq 0$ one has $n \leq l+s$, which is a contradiction. If $l+s = 0$ holds it implies that $l = -s$, which is a contradiction.

On the other hand, if $(r+l)q \equiv r-s \pmod n$ holds, one obtains

$$(r+l)q \equiv r-s \implies lq \equiv -s \pmod n \\ \implies n \mid (lq+s).$$

Since $l, s \leq r-2$ and $r < q$ hold, if $lq+s \neq 0$ holds it follows that $lq+s < n$, which is a contradiction. If $lq+s = 0$ then $lq = -s$, which is a contradiction.

Thus all the q -ary cosets $\mathbb{C}_{[0]}, \mathbb{C}_{[1]}, \dots, \mathbb{C}_{[r-2]}$, are disjoint from each one of the q -ary cosets $\mathbb{C}_{[r]}, \mathbb{C}_{[r+1]}, \dots, \mathbb{C}_{[2r-2]}$, so $C_2 \subsetneq C_1$. Additionally, all the q -ary cosets $\mathbb{C}_{[0]}, \mathbb{C}_{[1]}, \dots, \mathbb{C}_{[r-2]}$, are mutually disjoint and all the q -ary cosets $\mathbb{C}_{[r]}, \mathbb{C}_{[r+1]}, \dots, \mathbb{C}_{[2r-2]}$, are also mutually disjoint.

From the BCH bound, the minimum distance of C_1 is greater than or equal to r because its defining set contains the sequence $0, 1, \dots, r-2$, of $r-1$ consecutive integers. Similarly, the defining set of the code C generated by the polynomial $h(x) = \frac{x^n-1}{g_2(x)}$ contains the sequence $r, r+1, \dots, 2r-2$, of $r-1$ consecutive integers and so, from the BCH bound, C also has minimum distance greater than or equal to r . Since the code C_2^\perp is equivalent to C , C_2^\perp also has minimum distance greater than or equal to r . Therefore, the resulting CSS code has minimum distance greater than or equal to r .

Next we compute the dimension of the corresponding CSS code. We know that the degree of the generator polynomial of

a cyclic code equals the cardinality of its defining set. Further, the defining set Z_1 of C_1 has $r-1$ disjoint cyclotomic cosets. Moreover, all of them (except coset \mathbb{C}_0) have two elements and so, Z_1 has $2(r-2)+1$ elements. Therefore, C_1 has dimension $k_1 = n - 2(r-2) - 1$. Similarly, C_2 has dimension $k_2 = 2(r-2) + 1$. Thus the dimension of the corresponding CSS code equals $n - 4(r-2) - 2$. Applying the CSS construction to the codes C_1 and C_2 , one can get quantum codes with parameters $[[n, n - 4(r-2) - 2, d \geq r]]_q$. ■

We illustrate Theorem 3.1 by means of a graphical scheme:

$$\begin{array}{c} \overbrace{\mathbb{C}_{[0]} \mathbb{C}_{[1]} \mathbb{C}_{[2]} \dots \mathbb{C}_{[r-2]}}^{C_1} \\ \underbrace{\hspace{10em}}_{C_2} \\ \overbrace{\mathbb{C}_{[r]} \mathbb{C}_{[r+1]} \dots \mathbb{C}_{[2r-2]}}^C \quad \underbrace{\mathbb{C}_{[a_1]} \dots \mathbb{C}_{[a_n]}}_{C_2} \end{array}$$

The union of the cosets $\mathbb{C}_{[0]}, \mathbb{C}_{[1]}, \dots, \mathbb{C}_{[r-2]}$ is the defining set of code C_1 ; the union of the cosets $\mathbb{C}_{[0]}, \mathbb{C}_{[1]}, \dots, \mathbb{C}_{[r-2]}, \mathbb{C}_{[a_1]}, \dots, \mathbb{C}_{[a_n]}$ is the defining set of C_2 , where $\mathbb{C}_{[a_1]}, \dots, \mathbb{C}_{[a_n]}$ are the remaining cosets in order to complete the set of all cyclotomic cosets. The union of the cosets $\mathbb{C}_{[r]}, \mathbb{C}_{[r+1]}, \dots, \mathbb{C}_{[2r-2]}$ is the defining set of C .

Corollary 3.1: Assume that all the hypothesis of Theorem 3.1 are valid. Then there exist quantum codes with parameters $[[n, n - 4(c-2) - 2, d \geq c]]_q$, where $2 \leq c < r$.

Proof: Choose C_1 be the cyclic code generated by the product of the minimal polynomials

$$M^{(0)}(x)M^{(1)}(x) \dots M^{(c-3)}(x)M^{(c-2)}(x)$$

and C_2 be the cyclic code generated by the product of the minimal polynomials

$$\prod_i M^{(i)}(x),$$

where $i \notin \{r, r+1, \dots, r+c-2\}$ and i runs through the coset representatives mod n . Proceeding similarly as in the proof of Theorem 3.1, the result follows. ■

Example 3.2: Consider that $q = 9$ and $n = 40$; then $\gcd(9, 40) = 1$, $8 \mid 40$ and $\text{ord}_{40}(9) = 2$. In this case we have $r = 5$. Theorem 3.1 asserts the existence of a quantum code with parameters $[[40, 26, d \geq 5]]_9$. Consider next $q = 11$ and $n = 30$. Let C_1 be the cyclic code generated by the product of the minimal polynomials $M^{(0)}(x)M^{(1)}(x) \dots M^{(6)}(x)$ and C_2 be the cyclic code generated by the product of the minimal polynomials $\prod_i M^{(i)}(x)$,

where $i \notin \{7, 10, 15, 16, 18, 19, 21\}$ and i runs through the coset representatives mod 30. Proceeding similarly as in the proof of Theorem 3.1, an $[[30, 8, d \geq 8]]_{11}$ quantum code can be constructed.

B. Construction II - Codes of Prime Length

In this subsection the attention is focused on cyclic codes of prime length. Among the contributions shown in this section,

we prove there exists at least one q -ary cyclotomic coset containing two consecutive integers (see Lemma 3.2). The main result is Theorem 3.4, which generates new families of good quantum codes with parameters $[[n, n - 2mx, d \geq x + 2]]_q$, where $m = \text{ord}_n(q)$. In order to proceed further, let us recall a well-known result from number theory:

Theorem 3.2: A linear congruence $ax \equiv b \pmod{m}$, where $a \neq 0$, admits an integer solution if and only if $d = \gcd(a, m)$ divides b .

Applying Theorem 3.2 we can prove Lemma 3.2:

Lemma 3.2: Assume that $q \geq 3$ is a prime power, $n > q$ is a prime number and consider that $m = \text{ord}_n(q) \geq 2$. Then there exists at least one q -ary cyclotomic coset containing two consecutive integers.

Proof: First, note that $\gcd(q, n) = 1$. In order to prove this lemma, it suffices to show that the congruence

$$xq \equiv x + 1 \pmod{n}$$

has at least one solution for some $0 \leq x \leq n - 2$ or, equivalently, the congruence $(q - 1)x \equiv 1 \pmod{n}$ has at least one solution for some $0 \leq x \leq n - 2$. We know that $\gcd(q - 1, n) = 1$ holds, because $n > q$ and n is a prime number. Additionally, one has $q - 1 \neq 0$. Therefore, from Theorem 3.2, the congruence $(q - 1)x \equiv 1 \pmod{n}$ has an integer solution x_0 . Applying the division algorithm for x_0 and n one has $x_0 = ns_0 + r_0$, where r_0 and s_0 are integers and $0 \leq r_0 \leq n - 1$. Since the congruence $(q - 1)x_0 \equiv 1 \pmod{n}$ holds then the congruence $(q - 1)r_0 \equiv 1 \pmod{n}$ also holds. Moreover, since the integer $n - 1$ does not satisfy the latter congruence, it implies the existence of, at least, one q -ary coset containing two consecutive integers, and the result follows. ■

Lemma 3.3: If the q -ary coset $\mathbb{C}_{[s]}$ contains two consecutive integers then the q -ary coset $\mathbb{C}_{[-s]}$ also contains two consecutive integers.

Proof: If the q -ary coset $\mathbb{C}_{[s]}$ contains two consecutive integers, namely, x and $x + 1$, then the q -ary coset $\mathbb{C}_{[-s]}$ contains the consecutive integers $-x - 1$ and $-x$, concluding the proof. ■

Theorem 3.3: Let $q \geq 3$ be a prime power, $n > q$ be a prime number and consider that $m = \text{ord}_n(q) \geq 2$. Assume that $\mathbb{C}_{[s]} \neq \mathbb{C}_{[-s]}$, where $\mathbb{C}_{[s]}$ is a cyclotomic coset containing two consecutive integers. Then there exist quantum codes with parameters $[[n, n - 2m, d \geq 3]]_q$.

Proof: First, note that $\gcd(q, n) = 1$. Then choose C_1 be the cyclic code generated by the minimal polynomial $M^{(s)}(x)$ and C_2 be the cyclic code generated by the product of the minimal polynomials $\prod_i M^{(i)}(x)$, where $i \neq -s$ and i runs through the coset representatives mod n . It is easy to see that the cosets $\mathbb{C}_{[s]}$ and $\mathbb{C}_{[-s]}$ contain m elements. Proceeding similarly as in the proof of Theorem 3.1, the result follows. ■

Theorem 3.4 given in the following is the main result of this subsection:

Theorem 3.4: Assume that $q \geq 3$ is a prime power, $n > q$ is a prime number and consider that $m =$

$\text{ord}_n(q) \geq 2$. Let $\mathbb{C}_{[s]}$ be the cyclotomic coset containing s and $s + 1$. Suppose that all the q -ary cosets $\mathbb{C}_{[s]}, \mathbb{C}_{[s+2]}, \dots, \mathbb{C}_{[s+r]}, \mathbb{C}_{[-s]}, \mathbb{C}_{[-s-2]}, \dots, \mathbb{C}_{[-s-r]}$, are mutually disjoint. Then there exist quantum codes with parameters $[[n, n - 2mr, d \geq r + 2]]_q$.

Proof: Let $q \geq 3$ be a prime power and $n > q$ be a prime number. Then one has $\gcd(q, n) = 1$. From Lemma 3.3, the coset $\mathbb{C}_{[-s]}$ also contains two consecutive integers, namely, $-s - 1$ and $-s$.

Consider that C_1 is the cyclic code generated by the product of the minimal polynomials

$$M^{(s)}(x)M^{(s+2)}(x) \dots M^{(s+r)}(x)$$

and C_2 is the cyclic code generated by the polynomial $g_2(x)$, that is the product of the minimal polynomials

$$g_2(x) = \prod_j M^{(j)}(x),$$

where $j \notin \{-s - r, \dots, -s - 2, -s\}$ and j runs through the coset representatives mod n .

From the BCH bound, the minimum distance of C_1 is greater than or equal to $r + 2$ because its defining set contains the sequence of $r + 1$ consecutive integers given by $s, s + 1, s + 2, \dots, s + r$. Similarly, the defining set of the code C generated by the polynomial $h_2(x) = (x^n - 1)/g_2(x)$, contains a sequence of $r + 1$ consecutive integers given by $-s - r, \dots, -s - 2, -s - 1, -s$. Again, from the BCH bound, C has minimum distance greater than or equal to $r + 2$. Since C is equivalent to C_2^\perp , it follows that C_2^\perp also has minimum distance greater than or equal to $r + 2$. Therefore, the resulting CSS code have minimum distance greater than or equal to $r + 2$. It is easy to see that each one of the cosets \mathbb{C}_z , where $z \in [1, n - 1]$, has cardinality m . Additionally, from hypothesis, all the q -ary cosets $\mathbb{C}_{[s]}, \mathbb{C}_{[s+2]}, \dots, \mathbb{C}_{[s+r]}, \mathbb{C}_{[-s]}, \mathbb{C}_{[-s-2]}, \dots, \mathbb{C}_{[-s-r]}$, are mutually disjoint. Thus C_1 has dimension $k_1 = n - mr$ and C_2 has dimension $k_2 = mr$, since there exist r disjoint q -ary cosets not contained in the defining set of C_2 , where each of them has cardinality m . Therefore, the dimension K of the corresponding CSS code equals $K = n - 2mr$. Since the cosets $\mathbb{C}_{[s]}, \mathbb{C}_{[s+2]}, \dots, \mathbb{C}_{[s+r]}, \mathbb{C}_{[-s]}, \mathbb{C}_{[-s-2]}, \dots, \mathbb{C}_{[-s-r]}$, are mutually disjoint, it follows that $C_2 \subsetneq C_1$. Applying the CSS construction to C_1 and C_2 , one obtains an $[[n, n - 2mr, d \geq r + 2]]_q$ code. ■

Example 3.3: To construct an $[[19, 13, d \geq 3]]_7$ code, consider $q = 7$, $n = 19$ and $m = 3$. The cosets are given by $\mathbb{C}_2 = \{2, 14, 3\}$ and $\mathbb{C}_5 = \{5, 16, 17\}$. Let C_1 be the cyclic code generated by the minimal polynomial $C_1 = \langle g_1(x) \rangle = \langle M^{(2)}(x) \rangle$ and C_2 generated by $g_2(x) = \prod_i M^{(i)}(x)$, where $i \notin \{5\}$ and i runs through the coset representatives mod 19. Then an $[[19, 13, d \geq 3]]_7$ quantum code can be constructed. Similarly, one can get quantum codes with parameters $[[13, 5, d \geq 3]]_5$, $[[31, 25, d \geq 3]]_5$, $[[71, 61, d \geq 3]]_5$, $[[13, 5, d \geq 3]]_8$, $[[13, 7, d \geq 3]]_9$, $[[41, 33, d \geq 3]]_9$, $[[19, 13, d \geq 3]]_{11}$ and so on.

Remark 3.1: Note that most of quantum codes constructed in the previous example are new, with exception of the $[[31, 25, d \geq 3]]_5$ code, that is comparable to the quantum

Hamming code of length 31. Concerning these new codes, since the length of them are different from the length of the quantum Hamming codes, we can not compare such codes. Almost all codes constructed in the following example are new:

Example 3.4: To construct an $[[41, 21, d \geq 5]]_9$ code, consider $q = 9$, $n = 41$ and $m = 4$. The cosets are given by $\mathbb{C}_3 = \{3, 27, 38, 14\}$, $\mathbb{C}_4 = \{4, 36, 37, 5\}$, $\mathbb{C}_6 = \{6, 13, 35, 28\}$, $\mathbb{C}_7 = \{7, 22, 34, 19\}$ and $\mathbb{C}_{16} = \{16, 21, 25, 20\}$.

Let C_1 be the cyclic code generated by the product of the minimal polynomials $C_1 = \langle g_1(x) \rangle = \langle M^{(3)}(x)M^{(4)}(x)M^{(6)}(x) \rangle$ and be C_2 the cyclic code generated by the product of the minimal polynomials $g_2(x) = \prod_i M^{(i)}(x)$, where $i \notin \{7, 16\}$ and i runs through the coset representatives mod 41. From the BCH bound, the minimum distance of C_1 is greater than or equal to 5, since its defining set contains the sequence 3, 4, 5, 6. Similarly, the defining set of the code C generated by the polynomial $h(x) = \frac{x^{41}-1}{g_2(x)}$ contains the sequence 19, 20, 21, 22 and so, from the BCH bound, C also has minimum distance greater than or equal to 5. Since C is equivalent to C_2^\perp , C_2^\perp also has minimum distance greater than or equal to 5. C_1 has dimension $k_1 = 29$ and C_2 has dimension $k_2 = 8$. Then an $[[41, 21, d \geq 5]]_9$ code can be constructed. Similarly, one can construct quantum codes with parameters $[[11, 1, d \geq 4]]_3$, $[[31, 19, d \geq 4]]_5$, $[[31, 13, d \geq 5]]_5$, $[[71, 51, d \geq 4]]_5$, $[[71, 41, d \geq 6]]_5$, $[[19, 7, d \geq 4]]_7$, $[[19, 3, d \geq 5]]_7$, $[[19, 3, d \geq 5]]_{11}$, $[[41, 25, d \geq 4]]_9$ and so on.

C. Construction III - Codes Derived from Steane's Construction

In this subsection we construct new families of quantum BCH codes of prime length by applying the nonbinary Steane's enlargement of CSS construction [11, Corollary 4]. These new families have parameters better than the parameters of the quantum BCH codes available in the literature. Let us recall the Steane's construction:

Corollary 3.2: [11, Corollary 4] Assume we have an $[N_0, K_0]$ linear code L which contains its Euclidean dual, $L^\perp \leq L$, and which can be enlarged to an $[N_0, K'_0]$ linear code L' , where $K'_0 \geq K_0 + 2$. Then there exists a quantum code with parameters $[[N_0, K_0 + K'_0 - N_0, d \geq \min\{d, \lceil \frac{q+1}{q} d' \rceil\}]]$, where $d = w(L \setminus L'^\perp)$ and $d' = w(L' \setminus L'^\perp)$.

Euclidean self-orthogonal cyclic codes can be derived from Lemma 3.4:

Lemma 3.4: [1, Lemma 1] Assume that $\gcd(q, n) = 1$. A cyclic codes of length n over F_q with defining set Z contains its Euclidean dual code if and only if $Z \cap Z^{-1} = \emptyset$, where $Z^{-1} = \{-z \bmod n \mid z \in Z\}$.

In Lemma 3.2 of Section III-B we have shown the existence of, at least, one q -ary cyclotomic coset containing two consecutive integers provided the code length is a prime number. In what follows we show how to construct good quantum codes of prime length by applying the q -ary Steane's construction. We begin by presenting an illustrative example:

Example 3.5: Assume that $n = 31$ and $q = 5$. From Lemma 3.2, there exists a cyclotomic coset containing at least two consecutive integers; here is the coset $\mathbb{C}_8 = \{8, 9, 14\}$. Let C be the cyclic code generated by the product of the minimal polynomials $C = \langle g(x) \rangle = \langle M^{(4)}(x)M^{(8)}(x) \rangle$. C has defining set $Z = \mathbb{C}_4 \cup \mathbb{C}_8 = \{4, 7, 8, 9, 14, 20\}$ and has parameters $[31, 25, d \geq 4]_5$. From Lemma 3.4, it is easy to check that C is Euclidean self-orthogonal. Furthermore, C can be enlarged to a code C' with parameters $[31, 28, d \geq 3]_5$, whose generator polynomial is $M^{(8)}(x)$. Applying Corollary 3.2 to C and C' one obtains an $[[31, 22, d \geq 4]]_5$ code.

Theorem 3.5: Let $q \geq 3$ be a prime power, $n > q$ be a prime number and consider that $m = \text{ord}_n(q) \geq 2$. Let $\mathbb{C}_{[s]}$ be the q -ary coset containing s and $s+1$ and consider that $Z = \mathbb{C}_{[s]} \cup \mathbb{C}_{[s+2]}$, where $\mathbb{C}_s \neq \mathbb{C}_{[s+2]}$. Assume also that $Z \cap Z^{-1} = \emptyset$ holds. Then there exist quantum codes with parameters $[[n, n - 3m, d \geq 4]]_q$.

Proof: We know that $\gcd(q, n) = 1$. Let C be the cyclic code generated the product of the minimal polynomials

$$C = \langle M^{(s)}(x)M^{(s+2)}(x) \rangle.$$

By hypothesis and from Lemma 3.4 we know that C is Euclidean self-orthogonal. C has parameters $[n, n - 2m, d \geq 4]_q$. Consider C' be the cyclic code generated by the minimal polynomial $M^{(s)}(x)$. We know that C' is an enlargement of C and has parameters $[n, n - m, d \geq 3]_q$. Since $m \geq 2$, then $k' - k = m \geq 2$, where k' denotes the dimension of C' and k denotes the dimension of C . Applying the q -ary Steane's construction to C and C' , since $\frac{q+1}{q} > 1$ holds one obtains an $[[n, n - 3m, d \geq 4]]_q$ code. ■

Theorem 3.5 can be generalized in the following way:

Theorem 3.6: Assume that $q \geq 3$ is a prime power, $n > q$ is a prime number and consider that $m = \text{ord}_n(q) \geq 2$. Let $\mathbb{C}_{[s]}$ be the cyclotomic coset containing s and $s+1$. Assume that $Z = \mathbb{C}_{[s]} \cup \mathbb{C}_{[s+2]} \cup \dots \cup \mathbb{C}_{[s+r]}$, where all the q -ary cosets $\mathbb{C}_{[s+i]}$, $i = 0, 2, 3, \dots, r$, are mutually disjoint, and suppose that $Z \cap Z^{-1} = \emptyset$. Then there exist quantum codes with parameters $[[n, n - m(2r - 1), d \geq r + 2]]_q$.

Proof: We know that $\gcd(q, n) = 1$. Let C be the cyclic code generated by the product of the minimal polynomials

$$M^{(s)}(x)M^{(s+2)}(x) \dots M^{(s+r)}(x).$$

Since $Z \cap Z^{-1} = \emptyset$ holds, it implies from Lemma 3.4 that C is Euclidean self-orthogonal. From hypothesis, all the q -ary cosets $\mathbb{C}_{[s]}, \mathbb{C}_{[s+2]}, \dots, \mathbb{C}_{[s+r]}$ are mutually disjoint, so C has dimension $k = n - mr$ and minimum distance $d \geq r + 2$. Thus C has parameters $[n, n - mr, d \geq r + 2]_q$. Let C' be the cyclic code generated by the product if the minimal polynomials

$$M^{(s)}(x)M^{(s+2)}(x) \dots M^{(s+r-1)}(x).$$

We know that C' is an enlargement of C and has parameters $[n, n - m(r - 1), d \geq r + 1]_q$. Since $m \geq 2$ then $k' - k = m \geq 2$, where k' denotes the dimension of C' and k denotes the dimension of C . Applying the Steane's construction to the codes C and C' one obtains an $[[n, n - m(2r - 1), d \geq r + 2]]_q$ code, as required. ■

Example 3.6: In this example we construct an $[[31, 16, d \geq 5]]_5$ quantum code. For this purpose we take $n = 31$ and $q = 5$; then $m = \text{ord}_n(q) = 3$. Let C be the cyclic code generated by the product of the minimal polynomials $M^{(4)}(x)M^{(6)}(x)M^{(8)}(x)$. It is easy to see that C is Euclidean self-orthogonal and has parameters $[31, 22, d \geq 5]_5$. Let C' be the cyclic code generated by the product of the minimal polynomials $M^{(4)}(x)M^{(8)}(x)$; C' has parameters $[31, 25, d \geq 4]_5$. Thus there exists an $[[31, 16, d \geq 5]]_5$ quantum code.

We next establish Theorem 3.7, an analogous to Theorem 3.1.

Theorem 3.7: Suppose that $q \geq 5$ is a prime power and $n > q$ is an integer such that $\gcd(q, n) = 1$. Assume also that $(q - 1) \mid n$ and $m = \text{ord}_n(q) = 2$ hold. Then there exist quantum codes with parameters $[[n, n - 4c, d \geq c + 2]]_q$, where $1 \leq c \leq r - 3$ and $r > 3$ is such that $n = r(q - 1)$.

Proof: We only proof the existence of an $[[n, n - 4(r - 3), d \geq r - 1]]_q$ code, since the constructions of the other codes are quite similar.

Let C be the cyclic code generated by the product of the minimal polynomials

$$M^{(r)}(x)M^{(r+1)}(x) \dots M^{(2r-3)}(x).$$

From Lemma 3.1 and from the proof of Theorem 3.1, we know that the q -ary cosets given by $\mathbb{C}_{[r]} = \{r\}, \mathbb{C}_{[r+1]} = \{r+1, r+q\}, \mathbb{C}_{[r+2]} = \{r+2, r+2q\}, \dots, \mathbb{C}_{[2r-3]} = \{2r-3, r+(r-3)q\}$ are mutually disjoint and each of them has two elements. Therefore, C has dimension $k = n - 2(r-3) - 1$ and minimum distance $d \geq r - 1$.

Let us prove that C is Euclidean self-orthogonal. In fact, if $(r+i) \equiv -(r+j) \pmod{n}$, where $0 \leq i, j \leq r-3$, it follows that $2r+i+j \equiv 0 \pmod{n}$. Since the inequality $2r+i+j < n$ holds because $q \geq 5$, one has a contradiction. On the other hand, if $(r+i)q \equiv -(r+j) \pmod{n}$ holds then

$$\begin{aligned} (iq+j)(q-1) &\equiv 0 \pmod{n} \implies \\ i(q^2-q) + j(q-1) &\equiv 0 \pmod{n} \implies \\ j(q-1) &\equiv i(q-1) \pmod{n}, \end{aligned}$$

where the latter congruence holds because $\text{ord}_n(q) = 2$. Then the unique solution is when $i = j$. Let us investigate this case. Seeking a contradiction, we assume that the congruence $(r+i)q \equiv -(r+i) \pmod{n}$ is true. Then one obtains

$$\begin{aligned} (r+i)q &\equiv -(r+i) \pmod{n} \implies \\ 2r+i(q+1) &\equiv 0 \pmod{n} \implies \\ r(q-3) &\equiv i(q+1) \pmod{n}. \end{aligned}$$

If $0 \leq i \leq r-4$, then

$$\begin{aligned} r(q-3) - i(q+1) &\geq \\ r(q-3) - (r-4)(q+1) &= \\ 4q - 4r + 4 &> 0, \end{aligned}$$

where the latter inequality holds because $r < q$ since we only consider nonprimitive BCH codes. Moreover, the inequality $r(q-3) - i(q+1) < n$ also holds, which is a contradiction. If $i = r-3$ then the congruence $r(q-3) \equiv (r-3)(q+1)$

\pmod{n} holds, that is, $4r \equiv 3(q+1) \pmod{n}$ holds. Since $r \mid (q+1)$ and $q+1 > r$ hold, it implies that $q+1 \geq 2r$ so, $3(q+1) - 4r \geq 2r > 0$. Moreover, the inequality $3(q+1) - 4r < n$ holds, which is a contradiction. Therefore, C is Euclidean self-orthogonal.

Consider C' be the cyclic code generated by the product of the minimal polynomials

$$M^{(r)}(x)M^{(r+1)}(x) \dots M^{(2r-4)}(x).$$

C' is an enlargement of C ; C' has dimension $k' = n - 2(r-4) - 1$ and minimum distance $d' \geq r - 2$. Since $m = 2$ then $k' - k = 2$, where k' denotes the dimension of C' and k is the dimension of C . We know that $\lceil \frac{q+1}{q} d' \rceil \geq r - 1$. Thus, applying the q -ary Steane's construction one has an $[[n, n - 4(r-3), d \geq r - 1]]_q$ quantum code, as required. ■

Recall that an $[[n, k, d]]_q$ code C satisfies the quantum Singleton bound given by $k + 2d \leq n + 2$. If C attains the quantum Singleton bound, i. e., $k + 2d = n + 2$, then it is called a quantum maximum distance separable (MDS) code. In the following two examples we construct quantum MDS-BCH codes:

Example 3.7: Applying Theorem 3.7 for $q = 9$ and $n = 40$ one has $r = 5$. Thus there exists an $[[40, 36, 3]]_9$ quantum MDS-BCH code. Analogously, applying Theorem 3.7 for $q = 11$ and $n = 60$ one obtains an $[[60, 56, 3]]_{11}$ quantum MDS-BCH code. Additionally, an $[[60, 48, d \geq 5]]_{11}$ and an $[[60, 52, d \geq 4]]_{11}$ quantum codes can be constructed.

D. Construction IV - Hermitian Self-Orthogonal BCH Codes

In this subsection we present the fourth proposed construction, which is based on finding good Hermitian self-orthogonal BCH codes. Let us recall some useful concepts.

Suppose that C is a linear code of length n over F_{q^2} . Then its Hermitian dual code is defined by $C^{\perp_H} = \{y \in F_{q^2}^n \mid y^q \cdot x = 0 \text{ for all } x \in C\}$, where $y^q = (y_1^q, \dots, y_n^q)$ denotes the conjugate of the vector $y = (y_1, \dots, y_n)$.

Lemma 3.5: [1, Lemma 13] Assume that $\gcd(q, n) = 1$. A cyclic code of length n over F_{q^2} with defining set Z contains its Hermitian dual code if and only if $Z \cap Z^{-q} = \emptyset$, where $Z^{-q} = \{-qz \pmod{n} \mid z \in Z\}$.

Lemma 3.6: [1, Lemma 17 c)] (Hermitian Construction) If there exists a classical linear $[[n, k, d]]_{q^2}$ code D such that $D^{\perp_H} \subset D$, then there exists an $[[n, 2k - n, \geq d]]_q$ stabilizer code that is pure to d . If the minimum distance d^{\perp_H} of D^{\perp_H} exceeds d , then the stabilizer code is pure and has minimum distance d .

Example 3.8: Let us start with an example of how Lemma 3.1 can be applied together the Hermitian construction in order to construct good codes. Assume that $q = 7$, $n = 144$, $m = 3$ and $r = 3$; the q^2 -ary cosets $\mathbb{C}_3, \mathbb{C}_6, \mathbb{C}_9$ and \mathbb{C}_{12} contain only one element. The other cosets necessary for the construction are $\mathbb{C}_4 = \{4, 52, 100\}$, $\mathbb{C}_5 = \{5, 101, 53\}$, $\mathbb{C}_7 = \{7, 55, 103\}$, $\mathbb{C}_8 = \{8, 104, 56\}$, $\mathbb{C}_{10} = \{10, 58, 106\}$, $\mathbb{C}_{11} = \{11, 107, 59\}$.

Let C be the cyclic code generated by the product of the

minimal polynomials

$$M^{(3)}(x)M^{(4)}(x)M^{(5)}(x)M^{(6)}(x)M^{(7)}(x) \cdot \\ \cdot M^{(8)}(x)M^{(9)}(x)M^{(10)}(x)M^{(11)}(x)M^{(12)}(x).$$

It is straightforward to show that C is Hermitian self-orthogonal and has parameters $[[144, 122, d \geq 11]]_{7^2}$. Thus, applying the Hermitian construction, one obtains an $[[144, 100, d \geq 11]]_7$ quantum code. Similarly one can construct quantum codes with parameters $[[144, 102, d \geq 10]]_7$, $[[144, 108, d \geq 9]]_7$, $[[144, 114, d \geq 8]]_7$, $[[144, 116, d \geq 7]]_7$, $[[144, 122, d \geq 6]]_7$, $[[144, 128, d \geq 5]]_7$, $[[144, 130, d \geq 4]]_7$ and $[[144, 136, d \geq 3]]_7$.

In what follows we establish the first main result of this subsection:

Theorem 3.8: Suppose that $q > 3$ is a prime power and $n > q^2$ is an integer such that $\gcd(q^2, n) = 1$. Assume also that $(q^2 - 1) \mid n$ and $m = \text{ord}_n(q^2) = 2$ hold. Then there exist quantum codes with parameters $[[n, n - 4(r - 2) - 2, d \geq r]]_q$, where r is such that $n = r(q^2 - 1)$.

Proof: Let C be the cyclic code generated by the product of the minimal polynomials

$$M^{(r)}(x)M^{(r+1)}(x) \dots M^{(2r-2)}(x).$$

We first show that C is Hermitian self-orthogonal. For this, consider the defining set Z of C consisting of the q^2 -ary cyclotomic cosets given by $\mathbb{C}_{[r]} = \{r\}$, $\mathbb{C}_{[r+1]} = \{r + 1, r + q^2\}$, $\mathbb{C}_{[r+2]} = \{r + 2, r + 2q^2\}$, \dots , $\mathbb{C}_{[2r-2]} = \{2r - 2, r + (r - 2)q^2\}$.

We know that $\gcd(q, n) = 1$ holds. From Lemma 3.5, it suffices to show that $Z \cap Z^{-q} = \emptyset$. Seeking a contradiction, we assume that $Z \cap Z^{-q} \neq \emptyset$. Then there exist i, j , where $0 \leq i, j \leq r - 2$, such that $(r + j)q^l \equiv -q(r + i) \pmod{n}$, where $l = 0$ or $l = 2$. If $l = 0$, one has $r + j \equiv -q(r + i) \pmod{n}$ and so $q(r + i) + r + j \equiv 0 \pmod{n}$. Since $q(r + i) + r + j < n$ and $q(r + i) + r + j \not\equiv 0 \pmod{n}$ hold, one has a contradiction. If $l = 2$, it implies that $(r + j)q^2 \equiv -q(r + i) \pmod{n}$ and since $\gcd(q^2, n) = 1$ and $rq^2 \equiv r \pmod{n}$ one obtains

$$\begin{aligned} (r + j)q^2 &\equiv -q(r + i) \pmod{n} \\ \implies r + jq^2 &\equiv -q(r + i) \pmod{n} \\ \implies (q + 1)r &\equiv -q(i + jq) \pmod{n} \\ \implies -q(i + jq)(q - 1) &\equiv 0 \pmod{n} \\ \implies n \mid q(i + jq)(q - 1) \\ \implies r(q + 1) \mid q(i + jq). \end{aligned}$$

Since $\gcd(r, q) = 1$ and $\gcd(q + 1, q) = 1$ hold it implies that $r(q + 1) \mid (i + jq)$, which is a contradiction because $i + jq < r(q + 1)$. Thus C is Hermitian self-orthogonal.

It is easy to see that each one of these cosets are mutually disjoint and, with exception of the coset $\mathbb{C}_{[r]}$, the other cosets have two elements. Thus C has dimension $k = n - 2(r - 2) - 1$. By construction, the defining set Z of C contains the sequence $r, r + 1, \dots, 2r - 2$, of $r - 1$ consecutive integers and, so the minimum distance of C is greater than or equal to r , that is, C is an $[[n, n - 2(r - 2) - 1, d \geq r]]_{q^2}$ code.

Applying the Hermitian construction to C one can get an $[[n, n - 4(r - 2) - 2, d \geq r]]_q$ quantum code, as desired. ■

Corollary 3.3: Suppose $q > 3$ is a prime power and $n > q^2$ is an integer such that $\gcd(q^2, n) = 1$. Assume also $(q^2 - 1) \mid n$ and $m = \text{ord}_n(q^2) = 2$. Then there exist quantum codes with parameters $[[n, n - 4c - 2, d \geq c + 2]]_q$, where $2 \leq c < r - 2$ and $n = r(q^2 - 1)$.

Proof: Let C be the cyclic code generated by the product of the minimal polynomials $M^{(r)}(x)M^{(r+1)}(x) \dots M^{(r+c)}(x)$. Proceeding similarly as in the proof of Theorem 3.8, the result follows. ■

The following theorem is the second main result of this subsection:

Theorem 3.9: Let $q \geq 3$ be a prime power, $n > q^2$ be a prime number and consider that $m = \text{ord}_n(q^2) \geq 2$. Let $\mathbb{C}_{[s]}$ be the cyclotomic coset containing s and $s + 1$. Assume that $Z = \mathbb{C}_{[s]} \cup \mathbb{C}_{[s+2]} \cup \dots \cup \mathbb{C}_{[s+r]}$, where all the q -ary cosets $\mathbb{C}_{[s+i]}$, $i = 0, 2, 3, \dots, r$, are mutually disjoint, and suppose that $Z \cap Z^{-q} = \emptyset$. Then there exist quantum codes with parameters $[[n, n - 2mr, d \geq r + 2]]_q$.

Proof: We know that $\gcd(q, n) = 1$ holds. Let C be the cyclic code generated by the product of the minimal polynomials

$$M^{(s)}(x)M^{(s+2)}(x) \dots M^{(s+r)}(x).$$

Since $Z \cap Z^{-q} = \emptyset$ holds, it follows from Lemma 3.5 that C is Hermitian self-orthogonal. From the BCH bound, the minimum distance of C is greater than or equal to $r + 2$. It is easy to see that the cosets $\mathbb{C}_{[s+i]}$, where $i = 0, 2, 3, \dots, r$, have m elements and they are mutually disjoint. Thus C has parameters $[[n, n - mr, d \geq r + 2]]_{q^2}$. Applying the Hermitian construction one can get an $[[n, n - 2mr, d \geq r + 2]]_q$ code. ■

We finish this subsection by showing how Lemma 3.2 works for constructing quantum MDS-BCH codes:

Example 3.9: Let us consider $q = 5$ and $n = 13$. Since $\gcd(13, 24) = 1$, the linear congruence $(q^2 - 1)x \equiv 1 \pmod{n}$ has a solution, so there exists at least one q^2 -ary coset containing two consecutive integers, namely, the coset $\mathbb{C}_{[6]} = \{6, 7\}$. Choose $C = \langle M^{(6)}(x) \rangle$. Since $\mathbb{C}_{[4]} \neq \mathbb{C}_{[6]}$, C is Hermitian self-orthogonal and has parameters $[[13, 11, d \geq 3]]_5$. Applying the Hermitian construction, an $[[13, 9, 3]]_5$ quantum MDS-BCH code is constructed. Similarly, we can also construct an $[[17, 13, 3]]_4$ and an $[[17, 9, 5]]_4$ quantum MDS-BCH code.

IV. CODE COMPARISONS

In this section we compare the parameters of the new quantum BCH codes with the ones available in the literature. The codes available in the literature derived from the q -ary Steane's construction are generated by the same method presented in [20, Table I] by considering the criterion for classical Euclidean self-orthogonal BCH codes given in [1, Theorems 3 and 5].

Let us fix the notation:

- $[[n, k, d]]_q$ are the parameters of the new quantum codes;
- $[[n', k', d']]_q = [[n', n' - 2m(\lceil(\delta - 1)(1 - 1/q)\rceil), d' \geq \delta]]_q$ are the parameters of quantum codes available in [1];

TABLE I
CODE COMPARISON

New CSS codes	CSS codes in [1]
$[[n, k, d]]_q$	$[[n', k', d']]_q$
$[[1093, 1079, d \geq 3]]_3$	$[[1093, 1065, d' \geq 3]]_3$
$[[71, 61, d \geq 3]]_5$	$[[71, 51, d' \geq 3]]_5$
$[[18, 2, d \geq 5]]_7$	—
$[[21, 9, d \geq 5]]_8$	—
$[[10, 2, d \geq 4]]_9$	—
$[[40, 30, d \geq 4]]_9$	$[[40, 28, d' \geq 4]]_9$
$[[40, 20, d \geq 7]]_9$	—
$[[30, 7, d \geq 8]]_{11}$	—
$[[61, 55, d \geq 3]]_{13}$	$[[61, 49, d' \geq 3]]_{13}$
$[[84, 74, d \geq 4]]_{13}$	$[[84, 72, d' \geq 4]]_{13}$
$[[84, 70, d \geq 5]]_{13}$	$[[84, 68, d' \geq 5]]_{13}$
$[[84, 66, d \geq 6]]_{13}$	$[[84, 64, d' \geq 6]]_{13}$
$[[91, 85, d \geq 3]]_{16}$	$[[91, 79, d' \geq 3]]_{16}$
$[[144, 126, d \geq 6]]_{17}$	$[[144, 124, d' \geq 6]]_{17}$
$[[144, 122, d \geq 7]]_{17}$	$[[144, 120, d' \geq 7]]_{17}$
$[[144, 118, d \geq 8]]_{17}$	$[[144, 116, d' \geq 8]]_{17}$
$[[127, 121, d \geq 3]]_{19}$	$[[127, 115, d' \geq 3]]_{19}$

TABLE II
CODE COMPARISON

New CSS codes	q -ary Steane's construction
$[[n, k, d]]_q$	$[[n'', k'', d'']]_q$
$[[19, 13, d \geq 3]]_7$	—
$[[13, 7, d \geq 3]]_9$	—
$[[19, 13, d \geq 3]]_{11}$	—
$[[61, 55, d \geq 3]]_{13}$	$[[61, 52, d'' \geq 3]]_{13}$
$[[91, 85, d \geq 3]]_{16}$	$[[91, 82, d'' \geq 3]]_{16}$
$[[127, 121, d \geq 3]]_{19}$	$[[127, 118, d'' \geq 3]]_{19}$
$[[13, 5, d \geq 3]]_5$	—
$[[13, 5, d \geq 3]]_8$	—
$[[13, 7, d \geq 3]]_3$	—
$[[43, 31, d \geq 3]]_7$	—
$[[73, 61, d \geq 3]]_9$	—
$[[1093, 1079, d \geq 3]]_3$	$[[1093, 1072, d'' \geq 3]]_3$

- $[[n'', k'', d'']]_q$ are the parameters of quantum BCH codes derived from the q -ary Steane's construction shown in [11, Corollary 4].

In Table I, the new codes are derived from Construction I; in Table II, the new CSS codes are derived from Theorem 3.3 in Construction II; Tables III and IV show the new codes derived from Theorem 3.4 in Construction II; Table V presents new codes derived from Construction III and Table VI shows the new codes derived from Construction IV.

Checking the parameters of the new quantum BCH codes tabulated, one can see that the new codes have parameters better than the ones available in the literature. In other words, fixing n and d , the new quantum BCH codes achieve greater values of the number of qudits than the quantum BCH codes available in the literature. As the referee observed, it is interesting to note that most of our codes of length larger than $q^2 + 1$ are new (even most of codes of length lower than $q^2 + 1$ are new); see Tables below.

TABLE III
CODE COMPARISON

New CSS codes	CSS codes in [1]
$[[n, k, d]]_q$	$[[n', k', d']]_q$
$[[31, 19, d \geq 4]]_5$	$[[31, 13, d' \geq 4]]_5$
$[[31, 13, d \geq 5]]_5$	$[[31, 7, d' \geq 5]]_5$
$[[19, 7, d \geq 4]]_7$	—
$[[19, 3, d \geq 5]]_7$	—
$[[73, 61, d \geq 4]]_8$	$[[73, 55, d' \geq 4]]_8$
$[[73, 55, d \geq 5]]_8$	$[[73, 49, d' \geq 5]]_8$
$[[73, 49, d \geq 6]]_8$	$[[73, 43, d' \geq 6]]_8$
$[[73, 43, d \geq 7]]_8$	$[[73, 37, d' \geq 7]]_8$
$[[13, 1, d \geq 4]]_9$	—
$[[19, 7, d \geq 4]]_{11}$	—
$[[19, 3, d \geq 5]]_{11}$	—
$[[41, 21, d \geq 5]]_9$	—
$[[11, 1, d \geq 4]]_3$	—
$[[71, 51, d \geq 4]]_5$	$[[71, 41, d' \geq 4]]_5$
$[[13, 1, d \geq 4]]_3$	—
$[[43, 19, d \geq 5]]_7$	—
$[[73, 49, d \geq 5]]_9$	—
$[[73, 31, d \geq 7]]_9$	—

TABLE IV
CODE COMPARISON

New CSS codes	q -ary Steane's construction
$[[n, k, d]]_q$	$[[n'', k'', d'']]_q: L, L'$
$[[31, 19, d \geq 4]]_5$	$[[31, 16, d'' \geq 4]]_5: [31, 22, 4]_5, [31, 25, 3]_5$
$[[31, 13, d \geq 5]]_5$	$[[31, 10, d'' \geq 5]]_5: [31, 19, 5]_5, [31, 22, 4]_5$
$[[73, 61, d \geq 4]]_8$	$[[73, 58, d'' \geq 4]]_8: [73, 64, 4]_8, [73, 67, 3]_8$
$[[73, 55, d \geq 5]]_8$	$[[73, 52, d'' \geq 5]]_8: [73, 61, 5]_8, [73, 64, 4]_8$
$[[73, 49, d \geq 6]]_8$	$[[73, 46, d'' \geq 6]]_8: [73, 58, 6]_8, [73, 61, 5]_8$
$[[73, 43, d \geq 7]]_8$	$[[73, 40, d'' \geq 7]]_8: [73, 55, 7]_8, [73, 58, 6]_8$
$[[19, 7, d \geq 4]]_{11}$	—
$[[19, 3, d \geq 5]]_{11}$	—
$[[41, 25, d \geq 4]]_9$	—
$[[41, 21, d \geq 5]]_9$	—
$[[11, 1, d \geq 4]]_3$	—
$[[71, 51, d \geq 4]]_5$	$[[71, 46, d'' \geq 4]]_5: [71, 56, 6]_5, [71, 61, 3]_5$
$[[43, 19, d \geq 5]]_7$	—
$[[73, 49, d \geq 5]]_9$	—
$[[73, 31, d \geq 7]]_9$	—

TABLE V
CODE COMPARISON

New codes (Construction III)	q -ary Steane's construction
$[[n, k, d]]_q$	$[[n'', k'', d'']]_q$
$[[31, 22, d \geq 4]]_5$	$[[31, 16, d'' \geq 4]]_5$
$[[31, 16, d \geq 5]]_5$	$[[31, 10, d'' \geq 5]]_5$
$[[19, 10, d \geq 4]]_7$	—
$[[73, 64, d \geq 4]]_8$	$[[73, 58, d'' \geq 4]]_8$
$[[73, 58, d \geq 5]]_8$	$[[73, 52, d'' \geq 5]]_8$
$[[13, 4, d \geq 4]]_9$	—
$[[40, 36, 3]]_9$ (MDS)	—
$[[40, 32, d \geq 4]]_9$	$[[40, 30, d \geq 4]]_9$
$[[19, 10, d \geq 4]]_{11}$	—
$[[60, 56, 3]]_{11}$ (MDS)	—
$[[60, 48, d \geq 5]]_{11}$	$[[60, 46, d \geq 5]]_{11}$
$[[60, 52, d \geq 4]]_{11}$	$[[60, 50, d \geq 4]]_{11}$
$[[71, 56, d \geq 4]]_5$	$[[71, 46, d'' \geq 4]]_5$

TABLE VI
CODE COMPARISON

New Hermitian Codes (Construction IV)	Hermitian Codes in [1]
$[[n, k, d]]_q$	$[[n', k', d']]_q$
$[[17, 13, 3]]_4$ (MDS)	
$[[17, 9, 5]]_4$ (MDS)	
$[[13, 9, 3]]_5$ (MDS)	
$[[312, 298, d \geq 5]]_5$	$[[312, 296, d' \geq 5]]_5$
$[[312, 294, d \geq 6]]_5$	$[[312, 292, d' \geq 6]]_5$
$[[312, 290, d \geq 7]]_5$	$[[312, 288, d' \geq 7]]_5$
$[[312, 286, d \geq 8]]_5$	$[[312, 284, d' \geq 8]]_5$
$[[312, 282, d \geq 9]]_5$	$[[312, 280, d' \geq 9]]_5$
$[[312, 278, d \geq 10]]_5$	$[[312, 276, d' \geq 10]]_5$
$[[312, 274, d \geq 11]]_5$	$[[312, 272, d' \geq 11]]_5$
$[[312, 270, d \geq 12]]_5$	$[[312, 268, d' \geq 12]]_5$
$[[144, 128, d \geq 5]]_7$	$[[144, 120, d \geq 5]]_7$
$[[144, 122, d \geq 6]]_7$	$[[144, 114, d \geq 6]]_7$
$[[144, 116, d \geq 7]]_7$	$[[144, 108, d \geq 7]]_7$
$[[144, 114, d \geq 8]]_7$	$[[144, 102, d \geq 8]]_7$
$[[144, 108, d \geq 9]]_7$	$[[144, 96, d \geq 9]]_7$
$[[144, 102, d \geq 10]]_7$	$[[144, 90, d \geq 10]]_7$
$[[144, 100, d \geq 11]]_7$	$[[144, 84, d \geq 11]]_7$

V. SUMMARY

We have presented four quantum code constructions generating new families of good nonprimitive non-narrow-sense quantum BCH codes. These new quantum codes have parameters better than the ones available in the literature. Additionally, these codes are generated algebraically and not by computational search.

ACKNOWLEDGMENT

I would like to thank the anonymous referee for his/her valuable comments and suggestions that improve significantly the quality and the presentation of this paper. I also would like to thank prof. Reginaldo Palazzo Jr. for useful discussions with respect to the first quantum code construction and Dr. J. H. Kleinschmidt for critical reading of the manuscript. Part of this work was presented in ISITA 2012, Honolulu-Hawaii. This research has been partially supported by the Brazilian agencies CAPES and CNPq.

REFERENCES

- [1] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. On quantum and classical BCH codes. *IEEE Trans. Inform. Theory*, 53(3):1183–1188, 2007.
- [2] A. Ashikhmin and E. Knill. Non-binary quantum stabilizer codes. *IEEE Trans. Inform. Theory*, 47(7):3065–3072, 2001.
- [3] J. Bierbrauer and Y. Edel. Quantum twisted codes. *J. Comb. Designs*, 8:174–188, 2000.
- [4] R. C. Bose and D. K. Ray-Chaudhuri. On a class of error correcting binary group codes. *Information and Control*, 3:68–79, 1960.
- [5] R. C. Bose and D. K. Ray-Chaudhuri. Further results on error correcting binary group codes. *Information and Control*, 3:279–290, 1960.
- [6] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over $GF(4)$. *IEEE Trans. Inform. Theory*, 44(4):1369–1387, 1998.
- [7] H. Chen, S. Ling, and C. P. Xing. Quantum codes from concatenated algebraic geometric codes. *IEEE Trans. Inform. Theory*, 51(8):2915 – 2920, 2005.
- [8] G. D. Cohen, S. B. Encheva, and S. Litsyn. On binary constructions of quantum codes. *IEEE Trans. Inform. Theory*, 45(7):2495–2498, 1999.
- [9] M. Grassl and T. Beth. Quantum BCH codes. In *Proc. X Int. Symp. Theor. Elec. Eng.*, pp. 207–212, Magdeburg, Germany, 1999.

- [10] M. Grassl, T. Beth, and M. Rötteler. On optimal quantum codes. *Int. J. Quantum Inform.*, 2(1):757–766, 2004.
- [11] M. Hamada. Concatenated quantum codes constructible in polynomial time: efficient decoding and error correction. *IEEE Trans. Inform. Theory*, 54(12):5689–5704, 2008.
- [12] A. Hocquenghem. Codes correcteurs derreurs. *Chiffres*, 2:147–156, 1959.
- [13] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inform. Theory*, 52(11):4892–4914, 2006.
- [14] G. G. La Guardia. Constructions of new families of nonbinary quantum codes. *Phys. Rev. A*, 80(4):042331 (1–11), 2009.
- [15] G. G. La Guardia and R. Palazzo Jr. Constructions of new families of nonbinary CSS codes. *Discrete Math.*, 310(21):2935–2945, 2010.
- [16] G. G. La Guardia. New quantum MDS codes. *IEEE Trans. Inform. Theory*, 57(8):5551–5554, 2011.
- [17] Z. Ma, X. Lu, K. Feng and D. Feng. On non-binary quantum BCH codes. *LNCSS*, 3959:675–683, 2006.
- [18] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.
- [19] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [20] A. M. Steane. Enlargement of Calderbank-Shor-Steane quantum codes. *IEEE Trans. Inform. Theory*, 45(7):2492–2495, 1999.
- [21] L. Xiaoyan. Quantum cyclic and constacyclic codes. *IEEE Trans. Inform. Theory*, 50(3):547–549, 2004.
- [22] D.-W. Yue and G.-Z. Feng. Minimal cyclotomic coset representatives and their applications to BCH codes and Goppa codes. *IEEE Trans. Inform. Theory*, 46(7):2625–2628, 2000.